



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to Commissioner of Patents and Trademarks, Washington, D.C. 20231 on November 22, 2002.

Marchen Lopez
Name

Applicant : Koichiro Ikudome, et al.
Application No. : 09/295,966
Filed : April 21, 1999
Title : USER SPECIFIC AUTOMATIC DATA
REDIRECTION SYSTEM
Grp./Div. : 3621
Examiner : Pierre E. Elisca
Docket No. : 34503/WWM/A522

RECEIVED
DEC 05 2002
GROUP 3000

APPELLANT'S BRIEF

Assistant Commissioner for Patents
Washington, D.C. 20231

Post Office Box 7068
Pasadena, CA 91109-7068
November 22, 2002

Commissioner:

This is an appeal from the Final Rejection, dated October 12, 2001, of the claims in the above-referenced application.

1. REAL PARTY IN INTEREST

The real party in interest is the assignee of the subject application, Auric Web Systems.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-29 are pending in the present application.

Claims 1-29 have been rejected in a final rejection, dated October 12, 2001 under 35 U.S.C. §102(b).

The claims on appeal are claims 1-29.

4. STATUS OF AMENDMENTS

Appellants submitted additional remarks in a response to the final rejection. This response did not amend any claims. The response was not deemed to overcome the rejections. *See*, Paper 14, dated October 22, 2002. There are no outstanding, unentered amendments.

5. SUMMARY OF INVENTION

The invention is an improved database system and method for redirecting and filtering Internet traffic. *Appellants' Specification* (hereinafter "Specification"), 1:10-11 (passages are indicated by page:line). One embodiment of the invention relates to a system and method including a database 206¹ with entries correlating each of a plurality of user IDs with an individualized rule set. A dial-up network server 102 receives user IDs from users' computers 100, and a redirection server 208 is connected to the dial-up network server 102 and a public network 110. An authentication accounting server 204 is connected to the database 206, the dial-up network server 102 and the redirection server 208. The dial-up network server 102 communicates a first user ID for one of the users' computers 100 and temporarily assigned network address for the first user ID to the authentication accounting server 204. The authentication accounting server 204 accesses the database 206 and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server 208. *Specification*, 4:8-13. Data directed toward the public network 110 from one of the users' computers 100 are processed by the redirection server 208 according the individualized rule set. *Specification*, 3:30-4:7.

One embodiment of the invention also redirects the data to and from the users' computers as a function of the individualized rule set. *Specification*, 3:26-28. In another embodiment, at least a portion of the rule set for a temporarily assigned network address is automatically modified or at least a portion of the rule set is modified while that rule set remains correlated to the temporarily assigned network address. *Specification*, 3:28-30.

¹All numerals refer to FIG. 2.

6. ISSUES

(I) Whether claims 1-29 are unpatentable under 35 U.S.C. § 102(b) over Horowitz, et al. (WO 96/05549).

7. GROUPING OF CLAIMS

For purposes of this appeal, the claims are grouped as follows and for the purposes of this appeal only, the claims within each group stand and fall together. The claims consist of four independent claims, claims 1, 8, 15, and 26. Claims 1 and 15 claim systems and claims 8 and 26 claim methods corresponding to those systems. For determining anticipation within the meaning of 35 U.S.C. § 102(b), the groups are:

Group I - 1-4, 7-11, 14

Group II - 5-6, 12-13

Group III- 15-29

8. ARGUMENT

A. GROUP I

Group I includes claims 1-4, 7-11 and 14. Independent claim 1 recites a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network; and an authentication accounting server connected to the database, the dial-up network server and the redirection server, wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server, wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

The Examiner has rejected independent claim 1 under 35 U.S.C. §102(b) as being anticipated by *Horowitz*. *Horowitz* is directed to a local network² remote access server. *Horowitz*, Abstract. Remote users, such as telecommuters, can dial directly into a remote access server³ that checks the remote users' IDs and passwords against a database. *Horowitz*, 3:15-28. The database also includes pre-programed access filters indicating to which of the known devices connected to the local network (e.g., other computers, printers, etc.) the user can have access. *Horowitz*, 3:32-4:5. The remote access server can then allow or block the user from access to a particular device.

Similar packet filtering is discussed in the Appellants' background section. Specifically, "packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device." *Specification*, 2:30-34. However, this disadvantage can be largely irrelevant on a local network because the devices and networks⁴ on which the access filters are based are relatively static and known by the network administrator. *Horowitz* teaches that the database is "maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof." *Horowitz*, 8:31-9:2. Such control over a constantly changing *public* network, such as the Internet, is not feasible.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). *Horowitz* neither expressly nor inherently discloses every limitation of claim 1. Specifically, *Horowitz* does not disclose the claim element, "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." The entirety of the Examiner's grounds for rejection with respect to this element is that the element is "disclosed by *Horowitz*, in the abstract, specifically wherein it is stated that the server also includes processing

²See, e.g., *Horowitz*, Abstract, 1:5-10 and 3:1-7.

³See *Horowitz*, 4:6-23.

⁴See *Horowitz*, 3:29-4:5.

Application No. 09/295,966

electronics which control the communication and network ports.” See Final Office Action, p. 3. In an advisory action,⁵ the Examiner essentially repeated this ground stating:

Applicant’s representative argues that Horowitz does not [disclose] any about ‘a system that control a user’s access to a public network’...However, the Examiner respectfully disagrees because Horowitz in the Abstract, specifically wherein it is stated that processing [electronics] which control the communication...see office action mailed on 10/12/2001.

For a finding of anticipation, “the identical invention must be shown in as complete detail as is contained in the ...claim.” *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989). However, nothing in the reference’s passage from the Abstract cited by the Examiner discloses any data directed to a public network.

Although not explicitly stated, the Examiner appears to be making an assumption that “communication and network ports” inherently direct data to a public network. First, *Horowitz* fails to inherently anticipate the claimed element. “Inherent anticipation requires that the missing descriptive material is ‘necessarily present,’ not merely probably or possibly present, in the prior art.” *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295 (Fed. Cir. 2002). While it is true that it is possible to use “communication and network ports” to direct data to a public network, “communication and network ports” are often used in systems without directing data to a public network. For example, two stand alone computers directly connected over a telephone line with modems or two computers connected to each other in a simple LAN have “communication and network ports” controlled by processing electronics, but do not direct data toward a public network. Appellants therefore submit that the missing description of “directing data toward a public network” falls far short of being “necessarily present” in *Horowitz*, as is required by *Trintec Indus., Inc. v. Top-U.S.A. Corp.*

Second, the specific “communication and network ports” disclosed in *Horowitz* do not expressly teach or suggest anything about public networks or directing data to a public network. The “communication and network ports” in the *Horowitz* abstract cannot be read in

⁵See, Paper No. 14, sent November 8, 2002.

Application No. 09/295,966

a vacuum. They must be read in the context of the *Horowitz* disclosure. The entirety of *Horowitz* that discusses these ports is as follows:

Referring now to FIG. 4, in one embodiment, the remote access server 16 includes electronics 38, a plurality of serial communication ports 40₁-40_N, and a plurality of network ports 42₁-42_N. The server 16 also can include a plurality of internal modems 44₁-44_N. The serial ports 40 and the network ports 42 are controlled by the electronics 38.

The electronics 38 include, in some embodiments, a powerful 16 MHz 68EC020 microprocessor and memory such as up to 1 megabyte of battery backed-up static random access memory (SRAM) and possible 64 kilobytes in an erasable programmable read only memory (EPROM).

Each of the serial communication ports 40 is for coupling with a communication device (e.g., the modem 26 of FIG. 1), or for coupling directly with the telephone lines 22, *to provide for communication with a remote computer (e.g., the remote computer 12 of FIGS 1 and 2)* over the telephone lines 22. A connecting cable can be used to couple a serial port 40 with the communication device or with the telephone lines. Each of the serial ports 40 can simultaneously be coupled to a different one of the plurality of remote computers so as to provide simultaneous access to a local computer network for each of the remote computers, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC)...

Each of the network ports 42 *is for coupling with a local computer network (e.g., the network 14 of FIGS. 1 and 2)*, via a connecting cable, to provide for communication with the network...In some embodiments, the server 16 includes three network ports 42, one for 10BaseT Ethernet, one for Thin Ethernet, and one for Thick Ethernet. In some other embodiments, the server 16 includes a single network port 42 for Token Ring. In some other embodiments, the server 16 includes a single network port 42 for use with Apple LocalTalk.

Horowitz, 16:24-17:14, 17:24-18:1 (emphasis added). As indicated in the emphasized portion of this disclosure, the "communications ports" provide communication with remote computers used to remotely access the network that includes the communication ports, not a public network. Similarly, the "network ports" are coupled to a local computer network, not a public network. Nowhere in this discussion is there any teaching or suggestion of a public network or the "communication and network ports" being connected to one, and, in fact, the entire disclosure is expressly directed to only a *private* network.

Application No. 09/295,966

As discussed above, the differences between public and private networks are important. In private networks, such as in *Horowitz*, all of the resources and services are known. Private networks are “maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof.” *Horowitz*, 8:31-9:2. All of the resources and services are known. Additionally, since these networks are “private,” they are not accessible to the public. In a public network, the available resources and services are unknown and constantly changing. *Horowitz* states that an object of its access filter is to provide “security features” and “restrict access to the network on a per-user basis.” Public networks are not secure and access is unrestricted. Because *Horowitz* fails to disclose the cited limitations either expressly or inherently, Appellants respectfully submit that claim 1 is not anticipated by *Horowitz*.

Independent claim 8 recites a method that corresponds to the system recited in claim 1. Appellants respectfully submit that claim 8 and its dependent claims 9-14 are therefore patentable over *Horowitz*. Appellants respectfully request that the rejections to claims 8-14 be withdrawn.

For all of the reasons stated above, Appellants respectfully submit that claim 1, its dependent claims 2-7, claim 8 and its dependent claims 9-14 are patentable over *Horowitz* and respectfully request that the rejection under §102 be withdrawn.

B. GROUP II.

Group II includes claims 5-6 and 12-13. Claims 5-6 and 12-13 recite systems and methods that redirect data to and from the users' computers via the redirection server as a function of the individualized rule set. The passages in *Horowitz* cited by the Examiner do not teach or suggest this limitation. Instead, these passages relate to only blocking or allowing access to the private network, or particular devices on the private network. *Horowitz*, Abstract, 9:20-29. The Appellants can find no teaching or suggestion anywhere in *Horowitz* of directing the data to or from the user to an alternate location based on the individualized rule set and the Examiner has not identified such teaching or suggestion.

Application No. 09/295,966

Appellants include an extensive discussion regarding redirection of data in their specification. *Specification*, 1:29-2:16. Redirection involves the server "directing" the user to another area of the network. If the user chooses on its own to try to access another, allowable area of the network, this is clearly not redirection by the server. *Horowitz*, therefore, does not disclose any server that redirects data, but rather only passively blocks or allows data. As this limitation is neither expressly or inherently present in *Horowitz*, Appellants respectfully request that the rejections to Group II be withdrawn. Additionally, Appellants submit that claims 5-6 and 12-13 are dependent on patentable independent claims 1 and 8, respectively, and should therefore be allowed. The difference between passive blocking and allowing data and the redirection in this group of claims also makes these claims patentably distinct from the claims in Group I, because the claims in Group I would cover passive blocking and allowing data.

C. GROUP III.

Group III includes claims 15-29. Independent claim 15 recites a system comprising a redirection server programed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network; and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address.

The Examiner has rejected independent claim 15 under 35 U.S.C. §102(b) as being anticipated by *Horowitz*. As discussed in relation to Group I, above, *Horowitz* contains no express or inherent teaching or suggestion of a public network, or a rule set with functions used to control passing between the user and a public network. Appellants therefore respectfully submit that claim 15 and its dependent claims 16-25 are allowable and request that their rejections be withdrawn.

Additionally, *Horowitz* contains no teaching or suggestion of "automated modification of at least a portion of the rule set correlated to the temporarily assigned network address." Although Appellant brought the absence of this element to the Examiner's attention in every

communication,⁶ the Examiner has failed to cite any teaching or suggestion in *Horowitz* that meets this element or respond to Appellants' argument in any way. Appellant respectfully submits that the Examiner has failed to show that claims 15-25 are expressly or inherently anticipated by *Horowitz*, and therefore requests that the rejections to these claims be withdrawn. The automated modification element also distinguishes the claims of Group III from the claims of Group I as even if the claims of Group I were anticipated by *Horowitz*, there would be no anticipation of the Group III claims because *Horowitz* does not disclose or suggest the automated modification element.

Independent claim 26 recites a method that corresponds generally to the system recited in claim 15. Appellants respectfully submit that claim 26 and its dependent claims 27-29 are therefore patentable over *Horowitz*. Specifically, the Examiner has not cited any portion of *Horowitz* as disclosing "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address." Appellants respectfully request that the rejections to Group III be withdrawn.

D. CONCLUSION.

A single prior art reference will anticipate a claim only if it expressly or inherently describes each and every limitation in the claim. *Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Regarding Group I, the reference cited by the Examiner in support of his 35 U.S.C. §102(b) rejection fails to expressly or inherently teach or suggest "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set." *Horowitz*, in fact, contains no teaching or suggestion of a public network at all, and is expressly related to only a private network. Regarding Group II, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "redirection of data to or from a user." Finally, regarding Group III, the Examiner has failed to show any teaching or suggestion in *Horowitz* of "modification of a

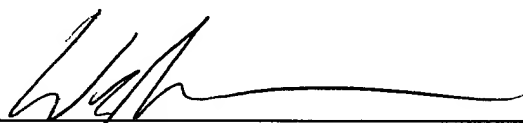
⁶See, Response to Office Action sent July 30, 2001 p. 7, Telephone conference of October 10, 2002, and Response to Office Action sent October 22, 2002 p. 3.

Application No. 09/295,966

rule set correlated to a temporarily assigned network address.” In fact, the Examiner has offered no argument or reference related to this claim element. Accordingly, the Examiner has failed to make out a prima facie case of anticipation and the issuance of a notice of allowance is appropriate.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By 
Wesley W. Monroe
Reg. No. 39,778
626/795-9900

9. APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

1. A system comprising:
 - a database with entries correlating each of a plurality of user IDs with an individualized rule set;
 - a dial-up network server that receives user IDs from users' computers;
 - a redirection server connected to the dial-up network server and a public network, and
 - an authentication accounting server connected to the database, the dial-up network server and the redirection server;wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;
- wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and
- wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.
2. The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.
3. The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.
4. The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

5. The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

6. The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

7. The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

8. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server, the method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

9. The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

10. The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

Application No. 09/295,966

11. The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

12. The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

13. The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

14. The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

15. A system comprising:
a redirection server programed with a user's rule set correlated to a temporarily assigned network address;
wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network; and
wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address.

16. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

Application No. 09/295,966

18. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user access.

19. The system of claim 15, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

20. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

21. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

22. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user access.

23. The system of claim 15, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

24. The system of claim 15, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

Application No. 09/295,966

25. The system of claim 24 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

26. In a system comprising a redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; the method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server.

27. The method of claim 26, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user access.

28. The method of claim 26, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user access.

29. The method of claim 26, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of:

receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

WWM/rah

MC PAS474061.2-* -11/22/02 9:18 PM